AU/ACSC/239/1999-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

INFORMATION OPERATIONS: MOVING FROM DOCTRINE TO EXECUTION

by

Seshagiri Munipalli, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major Tony R. Mullis

Maxwell Air Force Base, Alabama

April 1999

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Acknowledgments

I would like to acknowledge the assistance of my faculty research advisor, Lt Col (s) Tony R. Mullis, for his advice, support, and encouragement during this effort. His efforts to help me focus on this "Grand Canyon" topic were invaluable to me. I would especially like to thank Maj Tom Foltz, a fellow ACSC student, and Capt Frederick Baier of the Air Force Doctrine Center, for their review and invaluable comments on this paper. I also need to thank my peers in Seminars 27 and 30, whose daily humor and jest put this school in the proper perspective. Finally, I need to thank my family and more importantly my wife, Kristine. Without them, this project would not have been possible.

Abstract

The world is in a midst of an information technology revolution. The military force that best exploits and defends information and information systems will have the military advantage in the 21st Century battlespace. Much of the information and information systems that the military uses resides on the National Information Infrastructure (NII), which itself is inter-connected with the Global Information Infrastructure (GII). Consequently, vulnerabilities and threats to the GII and NII will impact not only military systems but also future military operations. Recognizing the potential of both the United States military and an adversary to exploit these vulnerabilities, the Joint Staff and the USAF have published their doctrines on information operations (IO). At the same time, the USAF is reorganizing its operational structure to a forward-deployed air expeditionary force. As a result, IO will play a greater role in enhancing the application of aerospace power against a future adversary. This research paper describes the roots of information superiority as envisioned in top-level visionary documents and the current IO doctrine. The research also discusses potential legal restrictions on IO and identifies some IO targets and threats. This paper also raises several issues with the USAF doctrine and recommends several steps for executing IO as the USAF transitions to an expeditionary force.

Chapter 1

Introduction

> *Information warfare, in its essence is about ideas and epistemology—big words meaning that information warfare is about the way humans think and more importantly, the way humans make decisions.*
>
> —George J. Stein
> *Cyberwar: Security, Strategy, and Conflict in the Information Age*

Background

In the past decade, the United States and the rest of the world have experienced an exponential increase in the amount of information available as the world transitions from the industrial age to the information age.[1] The United States is dependent upon networked information systems to conduct essential business such as power generation, financial transactions, international transportation, and global communication. This interdependent network is critical to U.S. economic competition in the global environment, but also makes this information infrastructure a potential center of gravity (COG). Through the interconnectivity offered by this seamless Global Information Infrastructure (GII), U.S. information systems are vulnerable to attack from anywhere and by anyone in the world.

The growing awareness of vulnerabilities of the GII has focused Department of Defense (DOD) attention on protecting our information and information systems and at the same time, creating a capability to exploit an enemy's information and information systems. This chapter traces the roots of information superiority from the viewpoint of the National Security Strategy (NSS) and Joint Staff and USAF vision documents. This chapter also describes the significance of information operations (IO) as currently embodied in the recent doctrine publications.

National Security Strategy

The need to protect and attack vital information and information systems is well documented in a broad array of strategic guidance documents ranging from the NSS to Joint and Service publications. The most recent NSS states that "threats to the national information infrastructure, ranging from cyber-crime to a strategic information attack on the United States via the global information network, present a dangerous new threat to our national security."[2] The NSS notes that "we must also guard against threats to our other critical national infrastructures—such as electric power and transportation—which increasingly could take the form of a cyber-attack in addition to physical attack or sabotage."[3] These threats come not only from traditional state actors, but also from transnational actors such as international crime organizations, narcotics traffickers and terrorists. The NSS also highlights foreign intelligence services adoption of these same technologies to access sensitive information by using the global information network to penetrate computer networks.[4]

Joint Vision 2010

Just as information and information systems are changing how the global community interacts, they are also changing the underlying concepts of national security and the way we apply force in future wars.[5] Information and the technology used to generate, transmit, process, store, and manipulate data may very well achieve an offensive or defensive advantage.[6] In *Joint Vision 2010*, the Chairman of the Joint Chiefs of Staff provides his vision on how the U.S. military forces will fight in the future. He provides the "conceptual template for how America's armed forces will…leverage technological opportunities to achieve new levels of effectiveness in joint warfighting."[7] Furthermore, *Joint Vision 2010* underscores the fact that "improvements in information and systems integration technologies will also significantly impact future operations."[8] The key to achieving "dominant battlespace maneuver" is through information superiority (i.e. the ability to provide continual and critical information to friendly forces while denying the same capability to the enemy).[9] *Joint Vision 2010* also recognizes that both offensive and defensive information operations are critical to information superiority.

Global Engagement

The USAF's *Global Engagement: A Vision for the 21st Century Air Force*, complements *Joint Vision 2010* by recognizing that "Information Operations…will grow in importance during the 21st Century."[10] Like *Joint Vision 2010*, *Global Engagement* recognizes that while offensive operations are important in order to exploit and deny information to the enemy, it is equally or more important to protect one's own information systems. *Global Engagement* states "the top IW [Information Warfare] priority is to defend our own increasingly information-intensive capabilities"[11] while continuing to develop offensive IW capabilities. *Global Engagement* acknowledges that information superiority will continue to remain one of the USAF's core competencies and suggests that information superiority is vital to the "control of air and space as a critical enabler for the Joint force."[12]

The above three documents clearly illustrate the importance of information superiority to future military operations. Both the Joint Staff and the USAF have taken the next step by incorporating the importance of information superiority and IO into their respective doctrine. Despite its emergence as a potential "revolution in military affairs," there are some underlying questions on whether the Joint community and the USAF is prepared for full realm of IO.

Definition of Research Topic

Significance of the Problem

The world is in the midst of an information revolution. The advancements in computing technologies are changing the basic power relationships of nation-states, politically, economically, and socially, but also militarily. In addition, the cost and size of computing technology are becoming cheaper and smaller. As a result, computers and other technology devices such as cellular phones and hand-held devices are now ubiquitous. The rapid expansion of these technologies has created a demand for information that is readily accessible and available to anyone at anytime or anyplace. This is readily seen in the dramatic increase in the use of the Internet, the single entity that has made information flow and exchange a global reality. The Internet has also expanded into third world and potential enemy countries such as China, Iran, and North Korea. Consequently, the information explosion also provides our adversaries with potential IO opportunities against our NII. Our enemies now have the ability to use information to ignite a Tofflerian "third wave war."[13]

Thesis

In order to exploit this new way of war and to combat the potential threat, the Joint Staff and the USAF have recently published their respective doctrines on IO. At the same time, the USAF is changing its war-fighting organization structure to meet future contingency needs and reduce operational tempo. For the Joint Force Commander (JFC) and the USAF, the Air Expeditionary Force (AEF) is the new way to deploy and employ aerospace power in the future.

However, the Air Force doctrinal documents do not address an IO strategy either unilaterally or in support of the AEF. At the direction of senior leaders at the CORONA TOP 98, the Air Intelligence Agency (AIA) is establishing IO Flights (IOF) at various Numbered Air Forces (NAF) as an initial step towards meeting the intent of the doctrine documents. Given the lack of technical tools and legal restrictions imposed upon the military, the question is whether the IOF concept is sufficient to support a war or military operations other than war (MOOTW).

This research will review the IOF concept as envisioned by AIA. This paper will then propose additional steps that the Air Force must take in order to meet the intent of its doctrine and to be consistent with the Joint doctrine.

Notes

[1] Alvin and Heidi Toffler*, War and Anti-war: Survival at the Dawn of the 21st Century*, (New York: Little, Brown, and Company, 1993), 9.

[2] The White House, *A National Security Strategy for a New Century*, October 1998, 6.

[3] Ibid.

[4] Ibid., 7.

[5] Douglas H. Dearth, "Information War: Rethinking the Application of Power in the 21st Century," *Military Intelligence*, January-March 1997, 11.

Notes

[6] Major Keith D. Anthony, "Information Warfare: Good News and Bad News," *Military Intelligence*, January-March 1997, 31.

[7] Joint Chiefs of Staff, *Joint Vision 2010*, Washington, D.C., 1996, 1.

[8] Ibid., 13.

[9] Ibid., 16.

[10] Department of the Air Force*, Global Engagement: A Vision for the 21st Century Air Force*, Washington, D.C., 1997, 14.

[11] Ibid.

[12] Ibid., 10.

[13] Toffler and Toffler, 9.

Chapter 2

Doctrine

> *Cyberwar is not merely a new set of operational techniques. It is emerging as a new mode of warfare that will call for new approaches to plans and strategies, and new forms of doctrine and organization.*
>
> —John Arquilla and David Ronfeldt
> *Cyberwar is Coming*

Military doctrine shapes the armed forces strategy and ensures unity of effort between the Services, Joint Staff, and other governmental and non-governmental agencies. Joint Publication 1, *Joint Warfare of the Armed Forces of the United States*, states that "military doctrine presents fundamental principles that guide the employment of forces."[1] Joint Pub 1 further underscores the importance of doctrine by indicating that "joint doctrine offers a common perspective from which to plan and operate, and fundamentally shapes the way we think and train for war."[2] From the military perspective, doctrine provides the framework for achieving national objectives through the military instrument of power.

The USAF doctrine echoes a similar position. In the foreword to Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, the Chief of Staff of the Air Force, General Michael E. Ryan, writes, "doctrine must draw together the lessons of history…and our insights of the future."[3] AFDD 1 further states that doctrine is the "linchpin of successful military operations."[4]

This chapter describes the origins of current IO doctrine, i.e. command and control warfare (C2W) doctrine. This chapter also introduces the Joint Staff and USAF doctrine for IO. Both doctrinal publications are the key to planning for and employing IO across the spectrum of conflict.

Command and Control Warfare Doctrine

The C2W concept originally began in the late 1970s, when the DOD published the first directive on command, control, and communications countermeasures (C3CM) application. This directive called for the "integrated use of operational security, military deception, jamming, and physical destruction to attack enemy command, control, and communications (C3) systems while protecting similar friendly systems."[5] Until the start of the Persian Gulf War, revisions to the early directive emphasized effective C3 capability while denying the same to our adversary. The revisions also reflected the combined nature of future wars and mandated C3CM training at the joint and multinational levels.

The Persian Gulf War reflected a major shift in the application of the early doctrine. The war demonstrated the effective use of the C3CM pillars to conceal Coalition movements, deceive Iraqi military, and destroy/jam Iraqi C2 systems and communications nodes. The war also represented the first integrated use of psychological operations (PYSOP) with traditional C3CM functions to encourage the Iraqi military to surrender.[6] The Gulf War's integrated C2W strategy effectively cut off the "eyes and ears" of the enemy.

The end of the Persian Gulf War saw a need to document the lessons learned from using C3CM in conjunction with PYSOP. These lessons of the war were initially codified in the Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30, which gave rise to C2W.[7] In 1996, the Joint Staff published its doctrine focusing on C2W policy, planning, education, and employment.

Joint Publication (JP) 3-13.1, *Joint Doctrine for Command and Control Warfare*, defines C2W as "the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions."[8] Like its predecessors, C2W has both offensive and defensive aspects (i.e. C2-Attack and C2-Protect, respectively). The C2-Attack objective is separate the "head from the body" by degrading or destroying the enemy's C2 systems while the C2-Protect objective is to overcome the effects of the enemy's C2-Attack.[9] The C2W doctrine also describes a relationship between itself and IW. JP 3-13.1 states that "command and control warfare is an application of IW in military operations and is a subset of IW."[10] C2W offers the military commander "lethal and non-lethal means to achieve the assigned mission while deterring war or promoting peace."[11] Even early on, the Joint Staff considered C2W as an effective tool before the outbreak of traditional hostilities and once in hostilities, as the tactical application of a large-scale IW.

Joint Information Operations Doctrine

Joint Publication 3-13, *Joint Doctrine for Information Operations*, captures the joint perspective on IO and provides the "overarching operational guidance for information operations."[12] The Joint doctrine defines IO as "actions taken to affect adversary information and information systems, while defending one's own information and information systems."[13] The doctrine also mandates the integration of IO with other operations (air, land, sea, space, and special) in order to "affect the information-based process, whether human or automated."[14]

The doctrine recognizes that IO is applicable at the strategic, operational, and tactical levels of war and can be used both in war and in MOOTW. At the strategic level, IO (as part of the military instrument of power [IOP]) is used with the diplomatic and economic IOPs to affect an adversary's national power base while protecting similar elements within the United States. At the operational and tactical level, IO helps to achieve campaign or tactical objectives against enemy logistics, intelligence, C2, and other related systems. The Joint Staff states that IO makes a huge impact by acting as a "deterrent in peace and during the initial stages of crisis."[15]

Like joint C2W doctrine , the IO doctrine is broken down into two aspects: offensive IO and defensive IO. Offensive IO is the "integrated use of assigned and supporting capabilities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives."[16] It integrates OPSEC, PSYOP, military deception, physical attack, and electronic warfare. The doctrine identifies a new capability called special information operations (SIO). SIO includes computer network attack (CNA). However, SIO use requires extensive policy review and approval by NCA or combatant commanders due to the potential for massive destruction.

Defensive IO is "the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems."[17] Defensive IO centers on four interrelated processes: information environment protection, information attack detection, capability restoration, and attack response. Together, these four processes "ensure defense in depth."[18] When conducting defensive IO, planners are required to integrate offensive IO along with information assurance, education, intelligence support, counter-deception, counter-propaganda operations, public affairs, command information programs, and counter-intelligence. The doctrine recognizes the military's contribution to information assurance by investigating information system incidents and apprehending criminals.[19] This "Pandora's box" gives the military a role in not only protecting military information systems, but also public and commercial information infrastructures. The protection of the NII also presents legal challenges for military commanders.

From a planning perspective, offensive and defensive IO are part of both deliberate and crisis action planning. Campaign plans leverage joint, Service, interagency, and multinational processes and capabilities.[20] As part of the planning process, the combatant commander identifies a "release and execution authority"[21] to coordinate potential legal issues regarding IO employment. Due to the mass effects of certain IO tools, it's probable that the authority will remain at the unified command or national level.

Air Force Information Operations Doctrine

The foreword to AFDD 2-5, *Information Operations*, sets the stage for the USAF concept of IO:

> Information has long been an integral component of human competition—those with a superior ability to gather, understand, control, and use information has had a substantial advantage on the battlefield. History is replete with examples of how information has influenced political and military struggles—from the earliest battles of recorded history to current operations in Bosnia. The Air Force's vision…recognized this by identifying information superiority as one of the six Air Force core competencies. The execution of information operations in air, space, and

> increasingly, in "cyberspace" constitutes the means by which the Air Force does its part to provide information superiority to the nation, joint force commander, and Service component and coalition forces.[22]

Like Joint Staff doctrine, USAF doctrine also recognizes that IO is applicable throughout the spectrum of military operations. Further, the doctrine considers IO as a force enabler by "supporting commanders in determining the situation, assessing threats and risks, and making timely and correct decisions."[23] The Air Force considers the end objective of IO is "information spectrum occupation" similar to "air occupation" through aerospace operations.

The two pillars of IO are information-in-warfare (IIW) and IW. Figure 1 shows the USAF's IO construct. The document defines IIW as IO conducted to "provide global awareness throughout the range of military operations based on its integrated intelligence, surveillance, and reconnaissance assets; its information collection and dissemination activities; and its global navigation and positioning, weather, and communications capabilities."[24] IIW is the traditional intelligence process for understanding the enemy and shaping the battlespace. IIW applies to both war and MOOTW operations.

IW is "information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems."[25] The attack aspect of IW is conducted during a crisis or conflict while the defend aspect is inherent in the peace-war continuum. AFDD 2-5 also breaks down IW into two distinct but inter-related components: offensive counter-information (OCI) and defensive counter-information (DCI). Like offensive counter-air/space operations and defensive counter-air/space operations, OCI and DCI achieve information superiority over an adversary.

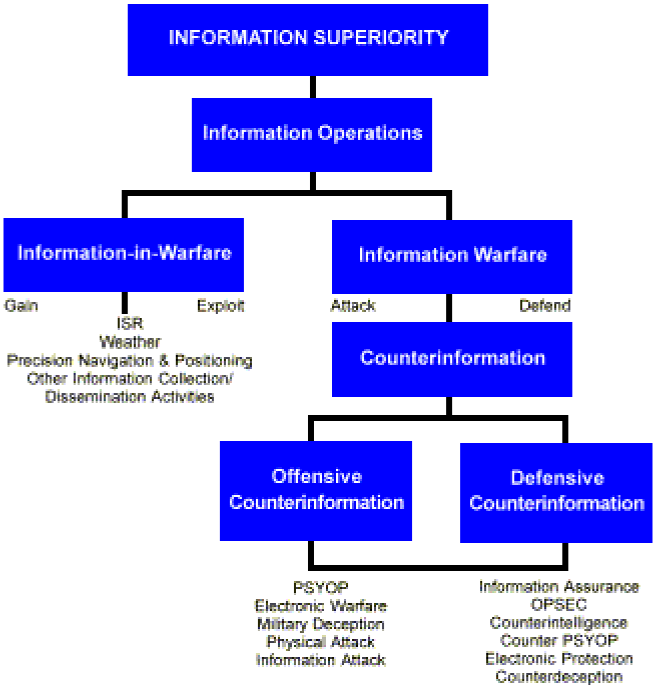

Figure 1. USAF Information Operations Construct[26]

OCI is "IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems."[27] The traditional C2 functions, PSYOP, EW, military deception, and physical attack fall under the OCI umbrella. Like the Joint C2W doctrine, the USAF doctrine reflects the lessons learned from the Persian Gulf War. One new function under OCI is a new capability called information attack (IA). IA is "activities taken to manipulate or destroy an adversary's information and information systems without necessarily changing visibly the physical entity within which it resides."[28] IA is similar to the Joint doctrine's SIO, specifically CNA.

DCI is "information operations conducted to protect and defend friendly information and information systems from the adversary."[29] The doctrine publication places information assurance, OPSEC, counter-deception, counter-intelligence, counter-PSYOP, and electronic protection under the DCI fold. The Joint doctrine recognizes the need to equally integrate offensive and defensive IO actions. Similarly, the USAF doctrine also stresses the need to coordinate OCI elements with DCI techniques. Unlike the Joint doctrine, the USAF places a greater emphasis on DCI by stating that "DCI is the Air Force's overall top priority within the information warfare area."[30] Military commanders are responsible for developing an effective DCI program, both in terms of posture and execution, within their commands. Further, the USAF doctrine is primarily focused on the military aspects of IO and does not address coordination with other government or non-governmental agencies including industry.

Air Expeditionary Force Concept

In 1998, the USAF devised a strategy to change its operational structure in order to reduce the operations tempo while continuing to meet contingency requirements. This new strategy calls for the establishment of 10 standing AEFs. Each AEF is a "force package" with elements of fighter, bomber, airlift, support personnel, aircraft, and equipment. The goal is to respond rapidly and effectively to any crisis or contingency situation in the world.[31]

Of the 10 AEFs, two are always ready to deploy for a 90-day period as a crisis response team. The other eight AEFs remain in their normal cycle of training or readiness inspection, but can deploy under normal war plans tasking. The end objective is for each AEF to deploy approximately every 15 months on a set schedule.[32]

While the expeditionary air force concept is not new, the AEF provides the JFC with a lethal mix of people and firepower. Since a "generic" AEF mix has both operations and support personnel within the air operations center (AOC), IO is critical to AEF employment. AFDD 2, *Organization and Employment of Aerospace Power*, tasks the Director of Operations and Plans within the AEF to "develop and coordinate a plan that integrates information operations to accomplish the joint force commander objectives."[33]

Summary

The Joint Staff and the Air Force have achieved a significant milestone in documenting how the combatant commander and the supporting commands will plan and organize for IO. The next step in the cycle is to establish a strategy for IO in support of strategic and operational objectives. While many of the IO functions are not new, CNA and/or IA present challenges to the military commanders. Both have the potential to create havoc and devastate an adversary beyond compare. The next chapter discusses the impact of the traditional law of armed conflict on this new capability.

Notes

[1] Joint Publication 1, *Joint Warfare of the Armed Forces of the United States,* 10 January 1995, vi.

[2] Ibid.

[3] Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, September 1997.

[4] Ibid., 1.

[5] Lt Col Norman B. Hutcherson, *Command and Control Warfare: Putting another tool in the War-fighter's Date Base*, Research Report no. AU-ARI-94-1 (Maxwell AFB, Ala.: Air University Press, September 1994), 2.

[6] Ibid., 4.

[7] Ibid., 5.

[8] Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, 7 February 1996, v.

[9] Ibid., I-4.

[10] Ibid., I-4.

[11] Ibid., I-5.

[12] Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, v.

Notes

[13] Ibid., I-9.
[14] Ibid., vii.
[15] Ibid., I-3.
[16] Ibid., II-1.
[17] Ibid., III-1.
[18] Ibid., III-1.
[19] Ibid., III-14.
[20] Ibid., V-1.
[21] Ibid., V-3.
[22] Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 5 August 1998.
[23] Ibid., 1.
[24] Ibid., 2.
[25] Ibid., 2.
[26] Ibid., 3.
[27] Ibid., 42.
[28] Ibid., 15.
[29] Ibid., 40.
[30] Ibid., 15.
[31] Bruce D. Callander, "The New Expeditionary Force," *Air Force Magazine* 81, no. 9 (September 1998): 54.
[32] Ibid., 56.
[33] Air Force Doctrine Document (AFDD) 2, *Organization and Employment of Aerospace Power*, 28 September 1998, 55.

Chapter 3

Information Operations and the Law

> *The worldwide information explosion provides new meaning to the expression "target-rich environment." The term does not do justice in today's information infrastructures and their value as targets. The challenge can be met by analyzing the adversary's processes and capabilities, including their technical characteristics and developing information weapons to attack at the optimum time.*
>
> —Brigadier General Grover Jackson, USAF, Retired
> *Air Intelligence Agency Spokesman Magazine*

The rapid explosion in information technology poses new challenges for international law, and specifically for international law addressing armed conflict. Satellites, cellular systems, computing technologies, and the Internet have not only linked the world into a seamless international network, but have done so at a pace that exceeds governmental regulation or international law and agreements. These new technologies have also allowed the military to create and deploy new armaments with unprecedented range, speed, and lethality.[1] Since information technologies can be used by the military to target an enemy's social and economic infrastructures, the law of armed conflict (LOAC) may apply to future military operations in the information realm. This chapter discusses the principles of LOAC, and how the legal and regulatory restrictions may impact IO.

Information as a Weapon

Joint Publication 3-13 defines information as "facts, data, or instructions in any form" or "the meaning that a human assigns to data."[2] But the question is whether information is a weapon itself. There are numerous historical examples of how the knowledge and understanding of information changed the course of a war. For example, in the Persian Gulf War, the Coalition used information to deceive and confuse the Iraqi's understanding of the battlefield.[3] During the war, information shaped the battlefield by externally affecting the Iraqi's information processing systems. The advances in computing technologies now make it possible to directly attack an enemy's internal information-based processing systems using IA tools. For the first time, information can be directly considered to be a weapon to achieve national security objectives. International law on how a nation can use or deny information in armed conflict is scarce. For now, LOAC as it applies to IO (in reality, CNA or IA) has to be extrapolated from other sources.

Law of Armed Conflict

International law is "the standard of conduct, at a given time, for states and other entities subject thereto. It comprises the rights, privileges, powers, and immunities of states and entities invoking its provisions, as well as the correlative fundamental duties, absence of rights, liabilities and disabilities." [4] The LOAC is the part of international law that regulates the conduct of armed hostilities by nations and primarily exists to reduce the effects of conflict and prevent unnecessary suffering by savagery or brutality.[5] It arose from a desire to lessen the effects of armed conflict.[6]

The LOAC is derived from several international treaties such as The Hague and Geneva Conventions as well as customary international law.[7] It applies regardless of whether or not a nation is formally at war with another state. Further, the LOAC applies to all armed conflicts between nation-states, but excludes civil wars or battles with transnational groups such as terrorists.[8] The USAF echoes a similar position by stating that its personnel will comply with LOAC during military operations and other armed conflicts, "regardless of how such conflicts are characterized."[9]

As mentioned above, the Hague Convention of 1907 addresses the use of armed force. The Convention divides the application of force into four basic principles: military necessity, proportionality, humanity and chivalry.

Military Necessity

The principle of military necessity "permits the use of regulated force that is not forbidden by international law and which is indispensable for securing the prompt submission of the enemy, with the least possible expenditures of life, time, and physical resources."[10] The principle requires that the user regulate the application of force. Military necessity also requires a military commander to estimate the amount of force required to capture or kill a combatant, while at the same time, ensuring that more force than necessary is not added. It also forces the commander to discriminate between legitimate military objectives and civilian objects.[11]

Humanity

The principle of humanity forbids military commanders to cause unnecessary suffering, injury or destruction that is not actually necessary for achieving legitimate military purposes.[12] It also outlaws the use of specific weapons that have been outlawed by international treaties such as certain chemical or biological weapons.[13]

Chivalry

The principle of chivalry compels a nation to wage war in accordance with well-recognized formalities and courtesies.[14] It exists primarily to make armed conflict less savage and more civilized for the individual combatant. It also attempts to outlaw treachery through illegal ruses such as faking a surrender or other acts of perfidy.[15]

Proportionality

The principle of proportionality acknowledges that the "application of armed force may result in physical destruction and personal injury/death to non-combatants or other non-military targets. It requires that the damage or death be limited to the extent consistent with the military necessity of the attack."[16] As such, military commanders are required to assess the potential for civilian destruction or death through an armed attack and the military necessity of the target before applying such force.[17]

Application of LOAC to Information Operations

If information is a weapon, similar to precision guided munitions or nuclear weapons, then LOAC applies across the board. Although it predates the development of IO techniques (specifically, IA or CNA), military commanders must consider LOAC in any potential conflict due to the ability to cause catastrophic damage through IA. Many questions on the proper application (both in terms of time and amount) of IA remain. For example, how can we ensure that information attacks are proportional when military and civilian power systems, financial networks, and communications systems are intertwined in a seamless network?[18] Fundamentally, when is an IA considered to be the use of armed force? This question requires the DOD to establish criteria for detecting and assessing an IA.

It's probably too early to determine the endless possibilities that may or may constitute an information attack. Clearly, the use of information weapons to produce results similar to a "hard kill" is equivalent to armed aggression.[19] On the other hand, the use of IO techniques to commit computer crimes, even from outside of a nation's territory, is not as an IA requiring a response in kind.[20] Consequently, before an IA is considered as "aggression by a foreign force," military commanders must ascertain the scale and nature of the attack along with the actors conducting the attack before responding militarily.[21] The challenge lies in determining the precise nature of the attack and establishing where in the cyberspace the attack occurred before resorting to the LOAC.

Summary

The use of IW by a state or by transnational actors such as terrorists may require a military response by the United States. While the criteria that may elicit a response by the military are unclear, any use of IO techniques to attain political or military objectives should conform to international law. This is especially important since computing technologies makes IA a potent technique to alter an adversary's power base or cause effects similar to weapons of mass destruction. Before any IA (either defensive or offensive) can take place, the military has to identify and characterize the nature of the attack before responding in kind. In order to utilize IO across the full spectrum of the conflict, it is necessary to understand the IW threats that may impact national and military infrastructures. The next chapter discusses the IW threats and the vulnerability of the United States to such threats.

Notes

[1] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, 30-31.

[2] Joint Publication 3-13, *Joint Doctrine for Information Operations*, GL-7.

[3] Alan D. Campen, *The First Information War*, (Fairfax, VA: AFCEA International Press, 1994), 1.

[4] Marjorie Millace Whiteman, *Digest of International Law*, vol.1 (Washington D.C.: Department of State, 1963), 1.

[5] Air Force Judge Advocate General School, *The Military Commander and the Law*, (Maxwell AFB, Ala.: Air University, 1998), 625.

[6] Air Force Policy Directive (AFPD) 51-4, *Compliance with the Law of Armed Conflict*, 26 April 1993, 1.

[7] Captain Robert G. Hanseman, "The Realties and Legalities of Information Warfare," *Air Force Law Review*, no. 42, 180.

[8] Ibid.

[9] Air Force Instruction (AFI) 51-401, *Training and Reporting to Ensure Compliance with the Law of Armed Conflict*, 19 July 1994, 1-1.

[10] Air Force Judge Advocate General School, 627.

[11] Hanseman, 181.

[12] Air Force Judge Advocate General School, 628.

[13] Hanseman, 182.

[14] Air Force Judge Advocate General School, 630.

[15] Hanseman, 182.

[16] Air Force Judge Advocate General School, 629.

[17] Hanseman, 182.

[18] Ibid., 183.

[19] Ibid., 184.

[20] Todd A. Morth, "Considering our position: Viewing Information Warfare as a use of force prohibited by Article 2(4) of the U.N. Charter," *Case Western Reserve Journal of International Law* 39, no. 567 (1998): 576.

[21] Ibid., 578.

Chapter 4

The Information Operations Threat

The electron is the ultimate precision guided weapon.

—John M. Deutch
Former Director, Central Intelligence Agency

As stated earlier, the United States is heavily dependent on global, networked systems for commerce, government, transportation, and financial transactions. More importantly, the U.S. military uses these same inter-connected, commercial systems to transmit financial information and personnel records data and to communicate basic orders between higher and lower echelons. Military commanders now receive information at an unprecedented speed and quantity due to advances in computer network systems and technologies. This dependence on national information-based systems raises potential vulnerabilities, which can be exploited by an adversary wishing to counter U.S. military objectives. According to Martin Libicki of the National Defense University (NDU), the United States is vulnerable to attack on its national information structure, and opines, "It must be assumed that any nation at war with the United States will attack military systems (especially logistics and mobilization systems) any way it can."[1]

This chapter discusses the potential threats to information-based systems and whether the United States is vulnerable to the newest form of IO (i.e. the Air Force's IA or Joint Staff's CNA). The United States is an "information dominant society" and as such, any future adversary will probably probe for vulnerabilities to our COGs and implement offensive IO measures in order to "cripple the our information based society from carrying out its information-dependent enterprises."[2]

What is the threat?

Joint Vision 2010 states that, "The U.S. must prepare to face a wider range of threats, emerging unpredictably, employing varying combinations of technology, and challenging us at varying levels of intensity."[3] The exponential growth and reliance on information and information-based systems makes IW a potential threat in the next century. Information attacks using computer-based systems is relatively inexpensive and offers a practical alternative to conventional attack by state and non-state actors. Consequently, radical groups and non-state terrorists can potentially cripple the United States. According to the CIA Director, George J. Tenet, "an adversary capable of implanting the right virus or accessing the right terminal can cause massive damage."[4]

Another aspect of IW is its anonymity. Computer network attacks (like a hacker invading a network for fun or with deadlier implications) can be waged from literally anywhere in the world. Once launched, IA or CNA is relatively difficult to detect. If detected, then it's even more difficult to assess the nature of the attack. If not assessed properly, the situation presents political and legal dilemmas for the DOD and national security decision-makers. Our adversaries may see any reluctance to act as a sanctuary from which to operate with impunity.[5] The Joint Staff underscores this dilemma and states that, "To get to the essence of the IW threat requires an understanding of three elements: identities and intentions of possible attackers; possible attack techniques and methods; and finally potential targets, extending from the strategic to the tactical levels."[6]

The Joint Staff publication, *Information Warfare: A Strategy for Peace…The Decisive Edge in War*, identifies several potential IW targets as shown in Figure 2. These types of targets are similar to Colonel John Warden's targets in his Five Rings model and are potentially the Unites States' COG for an enemy attack.

Leadership	**Military Infrastructure**	**Civil Infrastructure**	**Weapons Systems**
Key Personnel	Commanders	Communications (Links/Nodes)	Planes
ADP Support	C2 Communications Links	Industry	Ships
Strategic Communications	C2 Nodes	Financial	Artillery
Power Base	Intel Collectors	Populace	Air Defense

Figure 2. Examples of IW Targets[7]

Richard Power, a noted computer security expert, identifies ten infrastructure targets that may be attacked by IW means. Some potential U.S. targets are: (1) Culpepper Switch in Virginia which is responsible for all federal monetary transactions; (2) Alaska pipeline which handles 10 percent of the U.S. oil requirements; (3) Internet; (4) Time Distribution System; (5) Worldwide Military Command and Control System; (6) Electronic Switching System; (7) Air Force Satellite Control System; and (8) the National Photographic Interpretation System in Washington, D.C.[8]

AFDD 2-5 also presents examples of IW threats (and the weapons) which present a risk to information-based weapons and support systems. Figure 3 shows the various IW threats (i.e. weapons) that fall under four broad categories: compromise, deception/corruption, denial/loss, and destruction.

Compromise	**Deception/ Corruption**	**Denial/Loss**	**Destruction**
Malicious Code	Malicious Code	Malicious Code	Malicious Code
System Intrusion	Systems Intrusion	Systems Intrusion	Systems Intrusion
PSYOP	Military Deception	Lasers	Lasers
Intel Collection	Spoofing	Physical Attack	Physical Attack
Technology Transfer	Imitation	Nuclear and non-nuclear EMP	Nuclear and non-nuclear EMP
Software Bugs		Virus Insertion	Chemical/Biological Weapons
		Radio Frequency Jamming	Directed Energy Weapons

Figure 3. Information Warfare Threats and Weapons[9]

From the Air Force perspective, these IW weapons present a significant threat to weapons platforms such as the upcoming F-22 fighter, C4ISR systems, and to precision guided munitions. The area of most concern is with IA or CNA. It is rather easy for individuals to insert a computer virus or logic bomb to delay, degrade, or ideally destroy a weapon system. An adversary can use "insiders" or bribe individuals to insert an IW weapon during production and set the activation date to occur well into the future or after a specific act. The USAF considers these "internal threats" as the highest risk.[10]

Vulnerabilities of U.S. Information Systems

Despite disagreements on the nature of an IA or on the IO threat, there are numerous examples of attacks on DOD and national infrastructure systems. Computer hackers are invading computer systems daily. The Defense Information Systems Agency (DISA) estimates that in 1995 alone, up to 200,000 attacks occurred against defense-related systems.[11] In a DISA exercise, DISA personnel used computer hacking tools to attack about 25,000 DOD systems. The tools used to conduct the intrusions are readily available on the public market. They found that 98 percent of the system attacks were undetected.[12] Pentagon experts believe that outsiders probe military computers about 500 times a day with less than five percent being detected.[13]

How vulnerable is the U.S to this threat? According to the Defense Science Board Task Force on Information Warfare (Defense), a large measure of this is self-inflicted, in that, we have created our own vulnerabilities by placing critical capabilities on inadequately protected information systems. The study further notes that, "we have created a target-rich environment and the U.S. industry has sold globally much of the generic technology that can be used to strike these targets."[14] According to Clarence A. Robinson, editor of *SIGNAL* magazine, at least 122 nations have computer espionage programs, and the computer underground considers the DOD to be "easy pickings."[15]

As with DOD systems, there are similar concerns on the NII's vulnerability to an IA or CNA. The authors of *Critical Foundations: Protecting America's Infrastructures*, note potential vulnerabilities in five areas: information and communications, energy, banking and finance, physical distribution, and vital human services. The Chairman of the President's Commission on Critical Infrastructure Protection, Robert T. Marsh, writes that while the Commission did not foresee electronic disaster in the near future, it did find "widespread capability to exploit infrastructure vulnerabilities. The capability to do harm—particularly through information networks—is real; it is growing at an alarming rate; and we have little defense against it."[16]

Summary

From the information presented in this chapter, it is clear that there is an IA threat to not only military systems but also to the NII. The growing dependency on information and information-based technologies gives our adversaries several potential COGs for strategic attacks in any future conflicts. The military must consider the threat to information-based systems during IO planning and execution. If the military is to control the "information realm," the Joint Staff and the Services need to take the next step in combating the IA threat. The next chapter will examine the steps that the USAF must take to ensure that it is prepared to employ its own doctrine as it moves towards the expeditionary air force.

Notes

[1] Martin C. Libicki, "Protecting the United States in Cyberspace," in *Cyberwar: Security, Strategy and Conflict in the Information Age,* ed. Alan D. Campen et al. (Fairfax, VA: AFCEA International Press, May 1996), 12.

[2] Office of the Under Secretary of Defense for Acquisition and Technology, *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)* (Washington, D.C., November 1996), 2-1.

[3] Joint Chiefs of Staff, *Joint Vision 2010*, 11.

[4] Douglas Pasternak and Bruce B. Auster, "Terrorism at the Touch of a Keyboard," *U.S. News and World Report*, 13 July 1998, n.p.; on-line, Internet, 2 November 1998, available from http://www.usnews.com/usnews/issue/900713/13cybe.htm.

[5] Thomas G. Mahnken, "War in the Information Age," *Joint Forces Quarterly*, Winter 1995-96, 43.

[6] Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace…The Decisive Edge in War* (Washington, D.C., 1997), 9.

[7] Ibid., 13.

[8] Richard Power, "CSI Special Report on Information Warfare," *Computer Security Journal* 11, no. 2 (1995), 63-73.

[9] AFDD 2-5, *Information Operations*, 6.

[10] Ibid.

[11] Office of the Under Secretary of Defense for Acquisition and Technology, 2-15.

[12] Ibid.

[13] Douglas Waller, "Onward Cyber Soldiers", *TIME,* 146, no. 8, 21 August 1995, n.p.; on-line, Internet, 2 November 1998, available from http://cgi.pathfinder.com/time/magazine/archive/1995/950821/950821.cover.html.

[14] Office of the Under Secretary of Defense for Acquisition and Technology, 2-2.

[15] Clarence A. Robinson, Jr., "Defense Organization Safeguards War Fighter's Information Flow, *SIGNAL*, October 1995, 16.

[16] President's Commission on Critical Infrastructure Protection*, Critical Foundations: Protecting America's Infrastructures* (Washington, D.C., October 1997), i.

Chapter 5

Strategy to Execution

> *All that the AEF commanders need is the right information, at the right time, to help attack the right targets, in the right way.*
>
> —Robert Wall
> *Air Force Magazine*

The previous chapters have noted the United States growing dependency on the GII in order to compete in the global world. Any vulnerability inherent in the GII also impacts the NII and its DOD equivalent, the Defense Information Infrastructure (DII). The reliance on the GII makes IA or CNA a probable weapon of choice by our adversary. Our adversaries now have the technical ability to probe U.S.-based information systems and to launch an “information weapon” against these same systems from anywhere in the world, while remaining anonymous throughout the whole process. Consequently, the Joint Staff and the USAF must prepare to detect, assess, defend, and respond in kind to information attacks. This chapter discusses how the USAF should prepare for future battle in the information domain (i.e. the IA aspect of the IO doctrine). The first step is to develop a strategy for IO. Once the strategy is defined, the USAF should realign its IO doctrine so it is consistent with Joint doctrine. This chapter also presents several recommendations for organizing, training and equipping for IO.

Information Operations Strategy

Forward-deployed expeditionary air forces must operate effectively in any environment and against a wide range of potential adversaries. A strategy for IO is the first step by which the USAF can address how IO will enhance the myriad of aerospace functions. The end objective of the USAF's IO strategy is to achieve aerospace superiority through actions to deny, degrade, disrupt, or destroy the enemy's ability to command and control his forces. As future crises occur, national and theater-level decision-makers will probably seek an IO response or solution before resorting to purely armed actions. At the strategic level, the NCA may use IO along with other means to achieve national objectives by influencing or affecting an adversary's power structure. At the operational and tactical level, the AEF may conduct IO to achieve or support strategic objectives. All of these activities will require extensive coordination between the USAF and other government and non-governmental agencies in order to shape the strategic environment, respond to crises, and prepare for future conflicts.

The AEF can influence an adversary by shaping the political and economic environment through peacetime IO (e.g. PYSOP). The AEF can use public informational systems (i.e. media) to clearly articulate its mission and intent. If peacetime IO fails, the AEF can conduct pre-emptive IO (either IIW or IW) to deter adversaries from initiating hostile actions against the United States or its allies. In the pre-crisis stage, careful IO planning and execution may defuse a crisis and enhance the diplomatic and economic IOP. If deterrence fails, the AEF can conduct both OCI and DCI to shape the battlespace and prepare the way for armed action in order to achieve the JFC objectives. Once the crisis is resolved, selective IO elements will enhance negotiations and peace settlements favorable to the United States.

As described earlier, the information revolution presents both opportunities and vulnerabilities for the USAF and its new force package, the AEF. The AEF may operate in austere environments with limited host nation support and at the end of a tether originating from the United States. Its presence at and access to potential crisis areas may make it an operational and informational foundation for follow-on forces as part of the national or theater-level crisis response team. Consequently, the AEF's personnel, weapon systems, intelligence assets, and logistics infrastructure will require protection against potential IO threats.

In order to implement its IIW and IW strategy, the USAF must undertake several risk management actions. First, the USAF must develop IO databases on both friendly and enemy essential networks and systems to include the vulnerability of these systems to IO. By understanding the IO vulnerabilities and opportunities to both enemy and friendly systems, the AEF can influence the IO campaign planning and execution process in order to achieve national and theater objectives. Second, the USAF must strengthen its IO doctrine and ensure that appropriate IO-trained personnel, processes, and systems are deployed for IO prosecution from peace to war.

Refine the Air Force Doctrine

The USAF has taken the first step towards IO by publishing its doctrine. However, there are some potential issues that the USAF should to resolve in order to achieve unity of effort in IO. First and foremost are the terminology differences between the USAF doctrine and the Joint doctrine. The Joint doctrine delineates IO into two broad categories: offensive IO and defensive IO. The USAF equates these categories as OCI and DCI under an overarching umbrella called IW. While its understandable for the Air Force to equate OCI and DCI to its familiar role of OCA and DCA, the differences produce confusion and complexity in a joint operations environment. The USAF should refine its terms for the offensive and defensive applications of IO.

Second, the Air Force must identify organizational roles and responsibilities for IO at the major command or numbered air force (NAF) level. The doctrine mentions that an organic "IW Organization (IWO) will perform the duties and responsibilities of core and resident IW team members" as part of the Commander Air Forces (COMAFFOR) staff.[1] However the doctrine should clearly define these duties and responsibilities. Much of the thrust on IWO seems to be on the "defend" and not on "attack." AFDD 2-5 emphasizes this point by stating that "an IWO provides the COMAFFOR with real-time operational network intrusion detection and perimeter defense."[2] The doctrine also states that IWO teams can counterattack using physical or technical means,[3] but again this is a defensive response rather than an offensive attack. The doctrine also does not address procedures or responsibilities for technical counterattack. Technical means of counterattacking (i.e. IA) presents legal and moral challenges for the COMAFFOR. The doctrine should describe potential rules of engagement (ROE) during IO planning and execution.

Third, the doctrine does not identify a single executive agent for IO. The doctrine acknowledges that the Air Force Computer Emergency Response Team (AFCERT) is the "single point of contact…for computer security incidents and vulnerabilities."[4] While this enhances the defensive aspect of IW, there is not a corresponding lead organization for offensive IO. The relationship described in the doctrine between AFCERT and the major commands is exclusively on computer security (COMPUSEC), and IO is much more than just COMPUSEC. A logical choice is for the Air Force to identify AIA and specifically the Air Force Information Warfare Center as the lead agency for IO in the Air Force with the mission to coordinate IIW and IW tactics and procedures with the major commands. A single executive agent will also facilitate the legal and ROE considerations.

Finally, the doctrine needs to expand upon the current information environment and address the Service role in protecting the NII and the DII. Joint Pub 3-13 states that "Open and interconnected systems are coalescing into a rapidly expanding GII that includes the NII and DII."[5] Over 90 percent of defense communications and database applications take place on the NII.[6] While the DOD is not responsible for NII protection, the USAF can support national efforts by leveraging technology, procedures, and resources with industry partners and law enforcement officers.

Information Warriors

Martin Libicki and CDR James Hazlett of the NDU call for the DOD to create a separate and distinct Information Corps.[7] Libicki and Hazlett write that a separate corps with its own command structure will:

> …facilitate effective joint operations, promote the information revolution in warfare, unify the disparate information elements and give them an identity, create a common ethos for information warriors, and provide a unified interface with civilian information infrastructures.[8]

The Air Force has begun to establish IO Flights (IOF) in order to unify disparate IO elements and enhance unity of effort in IO planning.

Information Operations Flight

During CORONA TOP 98, several options were discussed for implementing IO at the NAFs. The outcome of CORONA 98 was to embed IO-trained personnel within various NAF directorates (A2, A3, and A6).[9] Further, the Air Force's only information warfare squadron (IWS), the 609th IWS, was stood down.

Currently, AIA is planning to establish an IOF at the 5th, 7th, 8th, 9th, 11th, and 13th NAF headquarters. Each IOF is headed by a field grade officer and is comprised of personnel from the intelligence, computer-communications, law enforcement, and public affairs career fields.[10] Each flight will have approximately 30-40 airmen with the bulk coming from AIA.

The IOF CONOP is still under construction by AIA. However, each IOF will "reach-back" to AIA headquarters for products and services.[11] The IOF responsibilities include IO database maintenance, enemy capability analysis, C2W target nominations, and C4ISR asset utilization in support of the NAF fighter wings.[12] Consequently, the IOF is responsible for both IIW (gain and exploit) and IW (attack and defend) functions.[13]

The Next Steps

The IOF is a first step in implementing the USAF doctrine. However, the initial CONOP raises potential issues during actual implementation. First, IOF personnel are distributed throughout various NAF headquarters directorates. Elements of the IOF will work on the NAF/A2, A3, and A6 staffs. This diversity of effort, which makes all three staffs responsible for IO, defeats unity of effort and cohesion. Each NAF directorate has competing requirements that may impact fusion of IO planning and execution within the

Air Tasking Order process. By organizing the IOF under a single directorate with responsibility for coordination between the NAF staffs and Joint and DOD-level agencies, the USAF can achieve economies of scale and focused IO planning and execution during the spectrum of conflict. It's also interesting to note that while AFDD 2-5 indicates that either the IWO or an IW team on the COMAFFOR staff will handle IW duties with intelligence support, AFDD 2 does not assign the A-2 any responsibility for either IW or IIW.[14] The USAF needs to correct this discrepancy.

The USAF also needs to accelerate the development of IO modeling and simulation tools, especially on IA. IO tools provide the combatant commander with a range of non-lethal and lethal options to achieve the strategic objectives. AIA is currently developing the Information Operations Planning Tool (IOPT), an advanced technology demonstration tool. The focus of IOPT is on attacking an adversary's Integrated Air Defense System.[15] AIA should expand IOPT to include an adversary's NII. The tools should also model the effects of an IA or CNA against the United States' NII and DII. AIA must also accelerate the development of modeling and simulation tools for training IO warriors and to exercise IO capabilities. AIA has taken initials steps to train and certify personnel for duty with the IOF by establishing an IO school at Hurlburt Field, Florida.[16]

Finally, the USAF must leverage advances in technology with industry partners. As computing hardware and software memory double every 18 months, the USAF must be able to exploit and defend against vulnerabilities resident in new information based systems. A possible solution is to establish an IO reserve force comprised of industry experts. During crises or war, these "civilian IO warriors" can protect the United States national infrastructures while probing for an adversary's infrastructure vulnerabilities.

Summary

The USAF must be prepared to defend against and execute IW. This chapter addressed several shortfalls in the current IO doctrine. The USAF must resolve these shortfalls in order to execute IO in support of joint operations. This chapter also addressed the AIA's IOF concept and provided some recommendations for IO modeling and simulation in support of JFC's objectives. The next chapter will summarize the thrust of this research paper.

Notes

[1] AFDD 2-5, *Information Operations*, 31.

[2] Ibid.,35.

[3] Ibid.,34.

[4] Ibid.,35.

[5] Joint Publication 3-13, *Joint Doctrine for Information Operations*, I-13.

[6] Joint Chiefs of Staff, *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations*, 3rd Edition (Washington, D.C., 17 September 1997), 1-7.

[7] Martin C. Libicki and James A. Hazlett, "Do We Need An Information Corps?" *Joint Force Quarterly*, Autumn 1993, 89.

[8] Ibid.

[9] 67th Operational Support Squadron, talking paper, subject: Info Ops Cadre Embedding, 3 August 1998.

[10] Ibid.

[11] 67th Operational Support Squadron, background paper, subject: Evolution of IO Embedding Concepts, 22 July 1998.

[12] Ibid.

[13] Ibid.

[14] AFDD 2, *Organization and Employment of Aerospace Power*, 54.

[15] Brigadier General (Retired) Grover Jackson, "Using Information as Weapons," *Air Intelligence Agency Spokesman Magazine* 38, no. 8 (August 1998): 6.

[16] First Lieutenant Matthew Mayberry, "AIA Intel Training Kicks Up A Notch," *Air Intelligence Agency Spokesman Magazine* 38, no. 9 (September 1998): 15-16.

Chapter 6

Conclusions

> *There will continue to be states or groups that oppose or threaten American interests and values or those of our friends and allies. Our recognition of these threats and challenges will continue to drive our national security efforts.*
>
> —Joint Vision 2010

Information Operations is becoming significant, both in the military as a whole and in the NII. For the military, "Information Warfare has emerged as a key joint war-fighting mission area."[1] In order to fully exploit this new way of war, both the Joint Staff and the USAF have published their respective doctrines on IO. The doctrines provide fundamental concepts and ideas on each entity's approach to IO.

Despite these recent publications, there are unresolved issues on the best means to organize, train, equip, and ultimately employ IO across the spectrum of conflict. The USAF especially needs to resolve terminology, organization, and relationship differences both internally and with the Joint community on IO.

But it's not all bad news. The USAF has taken several steps in the right direction. The IOF will energize and synergize IO planning and execution at the operational and tactical level. The USAF is also training IO warriors and developing IO modeling and simulation tools. However, there is yet more to be done. First, the USAF must develop IO techniques, tactics, and procedures (TTP) documents. The TTP documents will provide the foundation for ROE and legal considerations during IO exercises. Finally, the USAF must partner with industry to accelerate the development of not only IO modeling and simulation tools but also potential IA/CNA weapon systems. These tools are necessary to certify IO warriors and to provide an understanding of IA/CNA effects on an adversary's national power. These same tools will also help in modeling the effects of a potential attack on our NII and DII. The understanding of the effects of an IA or CNA is important for establishing the criteria for detection, assessment, and response. An IA or CNA effects-based criterion for the NII and DII will ensure the appropriate response by the proper United States agency.

Notes

[1] Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace…The Decisive Edge in War*, Preface.

Glossary

Command and control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (Joint Pub 3-13)

Command and control warfare (C2W). The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. (Joint Pub 3-13)

C2-Attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. (Joint Pub 3-13)

C2-Protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. (Joint Pub 3-13)

Computer network attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (Joint Pub 3-13)

Counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (Joint Pub 1-02)

Counterinformation. Counterinformation seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force. (AFDD 2-5)

Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Joint Pub 1-02)

Defense Information Infrastructure (DII). The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The Defense Information Infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. (Joint Pub 3-13)

Defensive counterinformation (DCI). Activities which are conducted to protect and defend friendly information and information systems. (AFDD 2-5)

Defensive information operations (DIO). The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (Joint Pub 3-13)

Electronic warfare (EW). Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (Joint Pub 3-13)

Global information infrastructure (GII). The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. (Joint Pub 3-13)

Information. 1. Unprocessed data of every description which may be used in the production of intelligence. 2. The meaning that a human as-signs to data by means of the known conventions used in their representation. 3. Facts, data, or instructions in any medium or form. (Joint Pub 1-02)

Information assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (AFDD 2-5)

Information attack. An activity taken to manipulate or destroy an adversary's information systems without visibly changing the physical entity within which it resides. (AFDD 2-5)

Information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (Joint Pub 3-13)

Information-in-warfare (IIW). Involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global navigation and positioning, weather, and communications capabilities. (AFDD 2-5)

Information operations (IO). Actions taken to affect adversary information and information systems while defending one's own information and information systems. The Air Force believes that in practice a more useful working definition is: *[Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare.*] {Italicized definition in brackets applies only to the Air Force. (AFDD 2-5, Joint Pub 3-13)

Information superiority (IS). The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. The Air Force prefers to cast "superiority" as a state of relative advantage, not a capability, and views IS as: [*That degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.*] {Italicized definition in brackets applies only to the Air Force and is offered for clarity.} (Joint Pub 3-13, AFDD 2-5)

Information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (Joint Pub 3-13)

Information warfare (IW). Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. The Air Force believes that, because the defensive component of IW is always engaged, a better definition is: [*Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems.*]. {Italicized definition in brackets applies only to the Air Force and is offered for clarity.} (Joint Pub 3-13, AFDD 2-5)

Military deception. Actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (Joint Pub 1-02)

National information infrastructure (NII). The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audiotape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. (Joint Pub 3-13)

Offensive counterinformation (OCI). Offensive IW activities which are con-ducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and in-formation systems. (AFDD 2-5)

Offensive information operations (OIO). The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision-makers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack. (Joint Pub 3-13)

Physical attack. The means to disrupt, damage, or destroy information systems through the conversion of stored energy into destructive power. (AFDD 2-5)

Probe. In information operations, any attempt to gather information about an automated information system or its on-line users. (Joint Pub 3-13)

Psychological operations (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (Joint Pub 1-02)

Special information operations (SIO). Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. (Joint Pub 3-13)

Vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (Joint Pub 3-13)

Bibliography

67th Operational Support Squadron. Talking paper. Subject: Info Ops Cadre Embedding, 3 August 1998.

67th Operational Support Squadron. Background paper. Subject: Evolution of IO Embedding Concepts, 22 July 1998.

Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine*, September 1997.

Air Force Doctrine Document (AFDD) 2. *Organization and Employment of Aerospace Power*, September 1998.

Air Force Doctrine Document (AFDD) 2-5. *Information Operations*, August 1998.

Air Force Instruction (AFI) 51-401. *Training and Reporting to Ensure Compliance with the Law of Armed Conflict*, 19 July 1994.

Air Force Instruction (AFI) 51-402. *Weapons Review*, 13 May 1994.

Air Force Judge Advocate General School. *The Military Commander and the Law*. Maxwell AFB, Ala.: Air University, 1998.

Air Force Policy Directive (AFPD) 10-20. *Air Force Defensive Counterinformation Operations*, 1 October 1998.

Air Force Policy Directive (AFPD) 51-4. *Compliance with the Law of Armed Conflict*, 26 April 1993.

Anthony, Major Keith D. “Information Warfare: Good News and Bad News.” *Military Intelligence*, January-March 1997, 31-32.

Arquilla, John and David Ronfeldt. *Cyberwar is Coming!* Bristol, PA: Taylor & Francis, 1993.

Callander, Bruce D. “The New Expeditionary Force.” *Air Force Magazine* 81, no. 9 (September 1998): [54-56].

Campen, Alan D. *The First Information War*. Fairfax, VA: AFCEA International Press, 1994.

Campen, Alan D., Douglas H. Dearth and R. Thomas Goodden. *Cyberwar: Security, Strategy and Conflict in the Information Age.* Fairfax, VA: AFCEA International Press, May 1996.

Dearth, Douglas H. “Information War: Rethinking the Application of Power in the 21st Century.” *Military Intelligence*, January-March 1997, 11-16.

Department of the Air Force. *Global Engagement: A Vision for the 21st Century Air Force,* Washington, D.C., 1997.

Hanseman, Captain Robert G. “The Realities and Legalities of Information Warfare.” *Air Force Law Review*, no. 42 (1997): [173-200].

Hutcherson, Lt Col Norman B. *Command and Control Warfare: Putting Another Tool in the War-Fighter’s Data Base*. Research Report no. AU-ARI-94-1. Maxwell AFB, Ala.: Air University Press, September 1994.

Jackson, Brigadier General (Retired) Grover. “Using Information as Weapons.” *Air Intelligence Agency Spokesman Magazine* 38, no. 8 (August 1998): [5-6].

Joint Chiefs of Staff. *Concept for Future Operations: Expanding Joint Vision 2010*. Washington, D.C., May 1997.

Joint Chiefs of Staff. *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations*, 3rd Edition. Washington, D.C., 17 September 1997.

Joint Chiefs of Staff. *Information Warfare: A Strategy for Peace…The Decisive Edge in War*. Washington D.C., 1997.

Joint Chiefs of Staff. *Joint Vision 2010*. Washington D.C., 1996.

Joint Publication 1. *Joint Warfare of the Armed Forces of the United States*, 10 January 1995.

Joint Publication 3-13. *Joint Doctrine for Information Operations*, 9 October 1998.

Joint Publication 3-13.1. *Joint Doctrine for Command and Control Warfare (C2W)*, 7 February 1996.

Libicki, Martin C. “Protecting the United States in Cyberspace.” *Cyberwar: Security, Strategy and Conflict in the Information Age.* Edited by Alan D. Campen, et al. Fairfax, VA: AFCEA International Press, May 1996.

Libicki, Martin C. and James A. Hazlett. “Do We Need an Information Corps?” *Joint Forces Quarterly*, Autumn 1993, 88-97.

Mahnken, Thomas G. “War in the Information Age.” *Joint Forces Quarterly*, Winter 1995-6, 39-43.

Mayberry, First Lieutenant Matthew. “AIA Intel Training Kicks Up a Notch.” *Air Intelligence Agency Spokesman Magazine* 38, no. 9 (September 1998): [15-17].

Morth, Todd A. “Considering our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter.” *Case Western Reserve Journal of International Law* 39, no. 567 (1998): [567-600].

Office of the Under Secretary of Defense for Acquisition and Technology. *Report of the Defense Science Board Task Force on Information Warfare–Defense (IW-D).* Washington, D.C., November 1996.

Pasternak, Douglas and Bruce B. Auster. “Terrorism at the Touch of a Keyboard.” *U.S. News and World Report*, 13 July 1998, n.p. On-line. Internet, 2 November 1998. Available from http://www.usnews.com/usnews/issue/900713/13cybe.htm.

Power, Richard. “CSI Special Report on Information Warfare.” *Computer Security Journal* 11, no. 2 (1995): [63-73].

President’s Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America’s Infrastructures*. Washington D.C., October 1997.

Robinson, Clarence A. Jr. “Defense Organization Safeguards War Fighter’s Information Flow.” *SIGNAL Magazine*, October 1995, 16-18.

Toffler, Alvin and Heidi Toffler. *War and Anti-war: Survival at the Dawn of the 21st Century*. New York: Little, Brown, and Company, 1993.

Wall, Robert. “Expeditionary Nerve Center.” *Air Force Magazine* 81, no. 8 (August 1998): 64-66.

Waller, Douglas. “Onward Cyber Soldiers.” *TIME Magazine* 146, no. 8, 21 August 1995, n.p. On-line. Internet, 2 November 1998. Available from http://cgi.pathfinder.com/time/magazine/archive/1995/950821/950821.cover.html.

White House. *A National Security Strategy for a New Century*. Washington, D.C., October 1998.

Whiteman, Marjorie Millace. *Digest of International Law*. Vol. 1. Washington D.C.: Department of State, 1963.

Air Command and Staff College
Maxwell AFB, Al 36112